REMARKS

This response is submitted in reply to the Final Office Action dated March 1, 2006. Claims 1-2, 5-15 and 17 are pending in the application. Claims 1-2, 7 and 14 have been amended. No new matter has been added by any of the amendments made herein. A Request for Continued Examination is submitted herewith. The Commissioner is hereby authorized to charge deposit account 02-1818 for any fees which are due and owing.

Applicants thank Examiner Simitoski for granting a telephonic interview on May 18, 2006. Examiner Simitoski and MacLane Key, Applicants' representative, participated in the call. While agreement was not reached, Examiner Simitoski indicated that the amendments made by this response are likely to overcome the art of record. Further, after Applicants' representative explained that Applicants intentionally refrained from limiting Claim 1 by specifying what is being encrypted, Examiner Simitoski indicated that the rejections under 35 U.S.C. §112, second paragraph are also overcome.

Accordingly, Applicants respectfully submit that at least for the reasons set forth below, the rejections have been overcome or are improper. Applicants respectfully request reconsideration of the patentability of claims 1-2, 5-15 and 17.

Claims 1-2, 5-15 and 17 were rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, regarding Claims 1-2, 7 and 14, the Office Action states that "it is unclear how, if the file registry information is creating by encrypting memory space specifying information, the file registry information could include the memory space specifying information in an unencrypted condition." Applicants respectfully disagree and submit that one of ordinary skill in the art would find the claim language clear; however, Applicants have amended the claims to make them more clear. Accordingly, Applicants respectfully request that these rejections be withdrawn.

The Office Action also states, "the limitation 'wherein said management section is adapted to create said access key information for each of the business organizations by encrypting based on said file key information and said user key information, wherein…' (last section) is unclear because there is nothing being encrypted 'based on said file key information…'." Applicants respectfully disagree with and traverse this rejection. Applicants

respectfully submit that the Office Action was incorrect when it claimed "nothing is being encrypted." As explained during the telephonic interview, for encryption to take place, something must be encrypted, and Claim 1, for example, requires "... said management sector is adapted to create said access key information for each of the business organizations by encrypting..." Applicants respectfully submit that one of ordinary skill in the art would understand that Applicants intended to not limit the scope of Claim 1 by specifying what must be encrypted and that Applicants intended the scope to broadly cover any encrypting that is based on the file key information and the user key information. Accordingly, Applicants respectfully request that these rejections be withdrawn.

Claims 1-2, 7-8, 11 and 14 were rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 4,710,613 to Shigenaga ("Shigenaga") in view of U.S. Patent No. 4,849,614 to Watanabe et al. ("Watanabe") in further view of U.S. Patent No. 5,161,256 to Iijima ("Iijima") in still further view of U.S. Patent No. 5,745,571 to Zuk ("Zuk") and in even further view of U.S. Patent No. 5,590,038 to Pitroda. Applicants respectfully maintain that there is insufficient motivation to combine these references to achieve the claimed invention; however, even if these references are combined, the combination of Shigenaga, Watanabe, Iijima, Zuk and Pitroda does not disclose, teach or suggest the elements of the claimed invention.

Claim 1 relates to an information processing system with a portable electronic device including means for processing information and a memory employed by a plurality of business organizations. The system includes a management sector including means for generating file registry information and access key information based on file key information and issuer key information processed by the management sector. The management sector is adapted to create the file registry information at least partly by encrypting memory space specifying information to at least partly produce an encrypted result. Further, the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result.

Shigenaga discloses an identification system for an integrated circuit card or IC card that is used in a card terminal. However, Shigenaga does not disclose or suggest file registry information that is created at least partly by encrypting memory space specifying information to at least partly produce an encrypted result, wherein the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result as

described in Claim 1. Shigenaga discloses encrypting data sent between a terminal and an IC card with an issuer or manufacturer key. However, even if the system of Shigenaga were to encrypt memory space specifying information before transporting the resulting encrypted information between the terminal and the IC card, the resulting encrypted information could not be the file registry information as described in Claim 1 because it would not include the memory space specifying information in an unencrypted condition in addition to the result produced at least partly by encrypting the file registry information.

Watanabe discloses a composite IC card for controlling information of a plurality of different enterprises where a memory is divided into a plurality of storage areas and where a code store section stores a plurality of codes necessary to access the storage areas of the card. However, like Shigenaga, Wantanabe does not disclose or suggest file registry information that is created at least partly by encrypting memory space specifying information to at least partly produce an encrypted result, wherein the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result as described in Claim 1.

Iijima discloses a method and system for allocating a file area in a memory area of an IC card or smart card. However, like Shigenaga, Iijima does not disclose or suggest file registry information that is created at least partly by encrypting memory space specifying information to at least partly produce an encrypted result, wherein the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result as described in Claim 1. The Office Action continues to state that Iijima discloses a management sector to generate file registry information, pointing particularly to Col. 4, Lines 38-59 and Fig. 11. However, Iijima does not disclose or suggest that the alleged file registry information (Fig. 11) is created by at least partly by encrypting memory space specifying information to at least partly produce an encrypted result or that the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result. Therefore, the alleged file registry information of Iijima cannot be the file registry information as described in Claim 1.

In an attempt to compensate for this deficiency, the Office Action appears to argue that the limitation could be interpreted to mean that the memory space information is ultimately

stored in an unencrypted condition. However, Applicants respectfully submit that ultimately storing memory space information in an unencrypted state as suggested by the Office Action would not disclose or suggest the file registry information including both the memory space information in an unencrypted state and the encrypted result produced at least partly by encrypting the memory space information.

Zuk discloses a cryptographic communications method and system for ensuring secure communications between a smart card and a terminal. Like Shigenaga, the data communicated between the smart card and terminal are encrypted and decrypted to securely transfer the data. However, also like Shigenaga, even if the system of Zuk were to encrypt memory space specifying information before transporting the resulting encrypted information between the terminal and the IC card, the resulting encrypted information could not be the file registry information as described in Claim 1 because it would not include the memory space specifying information in an unencrypted condition.

Pitroda discloses a universal electronic transaction card which is capable of serving as a number of different credit cards, bank cards, identification cards, employee cards and medical cards. However, it is respectfully submitted that Pitroda does not disclose or suggest file registry information that is created at least partly by encrypting memory space specifying information to at least partly produce an encrypted result, wherein the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result as described in Claim 1.

Accordingly, it is respectfully submitted that neither Shigenaga, Watanabe, Iijima, Zuk nor Pitroda, whether taken alone or in combination, disclose or suggest file registry information that is created at least partly by encrypting memory space specifying information to at least partly produce an encrypted result, wherein the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result as described in Claim 1.

Accordingly, for at these reasons, Claim 1 is patentably distinguished over the combination of Shigenaga, Watanabe, Iijima, Zuk and Pitroda and are in condition for allowance. For similar reasons, Claims 2, 7 and 14 and Claims 5-6, which depend from Claim 2, Claims 8-13, which depend from Claim 7, and Claims 15 and 17, which depend from Claim 14, are each

patentably distinguished over the combination of Shigenaga, Watanabe, Iijima, Zuk and Pitroda and are in condition for allowance.

Claims 5, 10, 15 and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shigenaga, Watanabe, Iijima, Zuk and further in view of "SMuG.0" by Canetti et al. ("Canetti"). Similar to Shigenaga, Watanabe, Iijima, Zuk and Pitroda, Canetti does not disclose or suggest file registry information that is created at least partly by encrypting memory space specifying information to at least partly produce an encrypted result, wherein the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result as described in Claims 5, 10, 15 and 17.

For at least these reasons, Claims 5, 10, 15 and 17 are each patentably distinguished over the combination of Shigenaga, Watanabe, Iijima, Zuk, Pitroda and Canetti and are in condition for allowance.

Claims 12-13 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Shigenaga, Watanabe, Iijima, Zuk and Pitroda and in further view of U.S. Patent No. 5,991,749 to Morrill Jr. ("Morrill"). Morrill is directed to the use of a cellular phone to conduct transactions. However, Morrill does not disclose or suggest file registry information that is created at least partly by encrypting memory space specifying information to at least partly produce an encrypted result, wherein the file registry information includes the memory space specifying information in an unencrypted condition and the encrypted result as described in Claims 12-13.

For at least these reasons, Claims 12-13 are each patentably distinguished over the combination of Shigenaga, Watanabe, Iijima, Zuk, Pitroda and Morrill and are in condition for allowance.

An earnest endeavor has been made to place this application in condition for allowance, and such allowance is courteously solicited. If the Examiner has any questions related to this Response, Applicant respectfully requests that the Examiner contact the undersigned.

Respectfully submitted,

BY _____
Thomas C. Basso (46,541)
Cust. No. 29175

Dated: May 26, 2006